Research Paper | Law | E-ISSN No : 2454-9916 | Volume : 9 | Issue : 7 | July 2023

AN ANALYTICAL STUDY OF CYBER-CRIME WITH SPECIAL REFERENCE TO INFORMATION TECHNOLOGY ACT, 2000

Nirav PrakashBhai Vithalani

Ph.D. Scholar, Department of Law, Saurashtra University, Rajkot

ABSTRACT

Under this research paper, the authors will try to express various cyber crimes in India with different statutory provisions in the Indian context. With the advancement of computers and various other technological devices, technology has been at the tip of fingers. But there is another major issue, that is, the issue of cyber crime and other IT related crimes has increased considerably as we are well aware of traditional crimes like theft, extortion, robbery, murder, etc. These crimes fall under the category of traditional crimes, in contrast to cyber-crime being a newly developed crime in which there is very little awareness among the people at large. It is worth noting that, these days the issue of cybercrime is very important. Especially in a country like India, where there is already little jurisprudence developed on cyber laws, crime rates have increased. Since the issue of cybercrime has arisen recently, more attention needs to be paid to deal with these newly developed crimes. With the advancement of technology and its use cyber frauds such as email spoofing, phishing, spamming, cyber defamation, Internet Relay Chat (IRC) etc. occur. There has been a huge increase. India lacks a proper legal regime to deal with cyber crimes. We have only one specific law to deal with cyber crimes, that is, the Information Technology Act, 2000

KEYWORDS: Cyber- Crime, Cyber space, Cyber- Offences, Information Technology Act 2000, Cyber laws

INTRODUCTION

The recent origin of cyber laws has given a way for various cyber crimes all over the world. As we see that man these days is completely dependent on information technology. Therefore, information technology has occupied a very prominent place in our daily lives. The term information technology is like an umbrella under which the term cyber crime comes. It is pertinent to note that, in the 21st century man cannot leave information technology. We all depend on information technology in one way or the other. Since information technology laws are of very recent origin, there has been little development of jurisprudence in the Indian context. Information technology is the application of competitors, telecommunications to retrieve and transmit data. According to section 2(1)(w)4 "information includes data, message, text, picture, sound, voice, code, computer programme, software and data base or microfilm or computer generated micro fish". If we see the definition of information, it is highly technical and beyond the understanding of a common man. Here we need to understand that we have many technical terms under Information Technology Act 2000 and cyber laws which are beyond the understanding of common man. Therefore, it is very necessary that cyber laws and related crimes are made available in a very clear and easy language that anyone can understand. The terms information technology and cyber space are closely related to each other. Here the term cyberspace is meant to describe the virtual world of computers. William Gibson is credited with coining the term. In layman's language the term cyber space is the place where individuals can interact, exchange ideas, express political opinion, sell and buy online and so on. Cyberspace has certain characteristics such as it is without boundaries, it regulates professional conduct on the Internet, it is an imaginary space with electronic data.

RESEARCH METHODOLOGY

The present research paper is based on Non- Empirical/Doctrinal research. In this research the author has used secondary data like articles, Information Technology Act 2000, Government reports and various other library resources.

OVERVIEW OF INFORMATION TECHNOLOGY ACT 2000

The Information Technology Act 2000 has 90 sections divided into thirteen chapters. The first chapter in this Act is devoted to the short title, extent, commencement and commencement of the Act. Apart from this, this chapter also includes explanation section. The second chapter deals with the power of the subscriber to authenticate the electronic record and electronic signature. Chapter three shows the importance of electronic governance. Chapter Four deals with the attribution, acknowledgment and transmission of electronic records. Chapter V contains provisions for securing electronic records and securing electronic signatures. The provisions of Chapter VI provide for regulation of Certifying Authorities, appointment of the Controller, their functions, powers and procedure for issue of Digital Signature Certificates. Chapter VII gives a detailed provision for obtaining Electronic Signature Certificate, suspension/revocation of Digital Signature Certificate. Chapter VIII lays down the duties of the subscriber for generation of key pair and electronic signature certificate and the conditions subject to which the digital signature certificate is accepted by the subscriber. Chapter IX contains statutory provisions for punishment and compensation for damage caused to computers and computer systems. Other provisions under this chapter deal with the procedure for adjudication of any dispute arising out of violation of any provision under the Information Technology Act, 2000. Chapter Ten of the Act contains sections 48-56 and provides for the establishment and composition of the Cyber Appellate Tribunal, qualifications. of the Chairperson and Members along with their terms and salaries. Chapter XI sets out the punishment for offenses under the Act. This part of the statute provides for punishment for sending objectionable messages through communication service. Section 66B under this part provides for punishment for dishonestly receiving stolen computer resource or communication equipment. Section 12 of the Act exempts intermediaries from liability in certain cases. Chapter Thirteen of the Act further elaborates on the miscellaneous provisions. Section 80 under this part deals with the power of police officer and other officers to enter and search. Section 81 further states that the Act shall have overriding effect over any other law. Finally section 81A makes provisions applicable to electronic cheques.[1]

CYBER CRIMES IN INDIA

Sextortion: The term 'sextortion' is very prominent in Indian cyber jurisprudence these days. As I can see in India there are many people who are victims of sextortion. In this form of new cyber crime, contact is made through social networking websites like Facebook, Instagram or dating apps or WhatsApp. After some conversation numbers are exchanged and the man gets a naked video call and becomes the bait. Recently a young man from Pune committed suicide after being fed up of blackmail through sextortion5. In one case, a 23-year-old youth committed suicide after being upset over a sexual assault case. The incident happened on 20 September 2022. The deceased woman had an Instagram friend who was a B.Com student at Garware College. After developing a close and personal friendship, the women asked the young man to undress as well. The accused allegedly threatened to post pictures and videos of the youth on social media and then demanded money from him. Threatening to reveal sexual photographs in order to force someone to do so is known as sextortion. These threats are made by both Internet strangers and former love partners who seek to harass, humiliate, and manipulate their victims. This commonly occurring crime can be seen all over the world through various sectors like education, government employment, police stations and more precisely the cyber world. This crime is for the greed of money. The more this crime increases in the society, the more the gambling of money increases. It is pertinent to note that the term sextortion increasingly refers to practices of 'revenge porn' among young people, where recordings of sexual activity are used for various forms of humiliation. In addition, blackmailing and retaliation are also the phenomena covered by the research that have received the most attention so far.

Cyber Stalking: Cyber stalking is basically stalking or harassing people through internet or computer resources. This could be the use of email, phone, text message, webcam, website or video. To be more precise in this cyber stalking, stalkers mainly track the location of the victim, monitor their every moment and social media, breach the data privacy of the person and then scare them. Moreover, stalkers usually threaten the person in such a way (morphing their pictures and threatening to leak them online, making rude and offensive comments, etc.) that the weak minded person is forced to take drastic steps. Which proves harmful for both. To the victim and her family as well. To elaborate

further this cyber stalking can also be divided into email stalking, internet stalking or computer stalking. On 6 June 2022, a woman from Nagpada was arrested for stalking, abusing and threatening other women on social media. And the accused was arrested under section 2927 for outraging the modesty of a woman.

Child Pornography: Pornography is an extreme form of pornography. This includes creating, sharing or accessing objects that sexually exploit a person through an Internet network. In India, viewing porn in a person's private space is not considered a crime, but showing nudity and obscenity, which are community norms, is strictly considered a crime. The thing which is affecting the society the most is cybercrime. The use of children in these pornographic videos is the biggest threat in the world

- **CYBER LAWS IN INDIA:**

Crime and society go hand in hand. There is no such society in which there is no crime or is free from crime. It is very important to make proper laws to reduce crime and deter criminal which can help in achieving a civilized society. These laws play an integral role in awakening and protecting the common citizens. Some Acts specify cyber laws such as Information Technology Act 2000 (herein referred to as IT Act), Indian Penal Code 1860 (herein referred to as IPC). This. The Act gives legal rights to electronic records and digital signatures, providing a foundation for electronic governance. Additionally, it defines cyber crimes and lays out the associated punishments. In order to control the issuing of digital signatures, the Act directed the creation of a Controller of Certifying Authorities.[2]

- **INFORMATION TECHNOLOGY ACT 2000:**

SECTIONS UNDER IT ACT	EXPLAINATION
Section 65	This section talks about tampering of the computer documents where any person who intentionally, willfully or consciously willfully or intentionally causes another to conceal, delete, or modify any computer source code used for a computer, computer programme, computer system, or computer network when the source code is required to be kept or maintained by law at the time it is in effect.
Section 66	This section is all about hacking of computer software. Anyone who intentionally damages, destroys, deletes, or modifies

Information Technology Amendment act 2008

	information stored on a computer belonging to a person or the public could receive a sentence of up to three years in prison, a fine of up to two lakh rupees, or both.
Section 66 -A	This section talks about punishment for the persons sending offensive messages. This includes - Any information or message that is offensive or contains threatening elements that is sent over a communication service. Any information that is given with the objective to annoy, inconvenience, danger, insult, obstructio n, hurt, or to incite hostility, hatred, or other negative feelings. Any electronic communication or email sent with the intent to annoy, trouble, mislead, or fool the recipient about the contents' origin. So, any person found guilty of such offences under this provision faces a maximum penalty of three years in jail and a fine.
Section 66 -B	This section talks about receiving a communication or computer resource that has been stolen dishonestly. Therefore, if you dishonestly obtain or retain a stolen computer resource or communication device and you are aware of the fact that it is stolen or you have reason to suspect that it is stolen, you may be subject to a jail sentence and/or a fine of up to one lakh rupees, or both.
Section 66 -C	This section is all about Identity theft. This crime is committed when someone uses other
	person's password, digital or electronic signature, or another unique form of identity. Therefore, anyone involved in such offences may receive a penalty that includes either a description for a duration that may extend up to 3 years in prison or a fine that may extend up to Rs. 1 lakh.
Section 66-D	This section talks about punishment for using a computer resource to commit personation fraud. – Any individual found guilty of personation fraud utilizing a communication device or computer resource faces a fine of up to one lakh rupees in addition to general or specific imprisonment for a term not to exceed three years.
Section 66-E	This section talks about privacy and violation. Anyone who violates someone's right to privacy by sending or taking images of their private spaces or private regions without their permission, whether knowingly or not, faces a maximum of three years in imprisonment or a fine of up to 2 lakh rupees, but not both.
Section 66-F	Section 66 F holds a great importance and talks about cyber terrorism. Those who purposefully put integrity, unity, sovereignty, or security in jeopardy or cause dread among the general public or any portion of the general public by I. Prohibiting anyone from using the resources of the computer.
	Making an attempt to gain unauthorised access to, break into, or use a computer resource. III. Introducing a computer contamination, and via such conducts causing or likely to cause any death or injury to a person, damage to property, or destruction of property, or disrupt ing or it is known that through such conduct it is likely to cause damage to the infrastructure for important information as defined in section 70 of the IT Act, or poses a threat to such infrastructure. B. By purposefully or knowingly attempting to access computer resources without authorization or going beyond what is permitted, and by engaging in such conduct, obtaining access to data, information, or computer databases that are restricted or limited for a variety of reasons related to national security or international relations, or to any restricted database, data, or information with reason to believe that those data, information may be used to cause injury.
Section 67	Punishment for publishing or transmitting obscene material in electronic form. –Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be
	punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description f or a term which may extend to five years and also with fine which may extend to ten lakh rupees. [12]

Section 67 -A	According to this clause, anyone who acts electronically or transmits or publishes sexually explicit material could receive a first -time offender punishment of up to five years in prison or a fine of up to ten lakh rupees. And in the event of a second conviction, the offender may be given a punishment for any classification that comprised up to 7 years in prison and a fine of up to 20 lakh rupees.
Section 67 -B	The focus of Section 67 -B is transmission or any person found guilty of transmitting or distributing any materials showing children engaged in sexual conduct in an electronic form faces a maximum term of five years in prison and a fine of 10 lakh rupees for a first offence. Additionally, if convicted again, offenders might rece ive sentences for any category that could last up to 10 lakhs in fines and sentences of up to 7 years.
Section 69	This clause gives the authority to direct the monitoring, decryption, or interception of any information using computer resources.

Information Technology Act 2000.

Section 70	This section is about securing entry to a secure system - Any computer, computer system, or computer network may be deemed a protected system by the competent government by publication in the Official Gazette. The individuals who are permitted to access protected systems may be approved by written order from the competent government. A person is breaking the law if they acquire access to, or try to secure access to, a protected system. Penalty: Up to ten years in prison, or/and a fine. [13]
Section 79	After a 2000 amendment, this law no longer exempts intermediaries and now specifies that if the following criteria are satisfied, the intermediary is not responsible for any third-party information data or communication link he makes availab le or hosts: (a) The intermediary's function is limited to offering access to a communication system used to transfer, temporarily store, or house information made available by third parties; (b) The communication is not started by the intermediary. Howe ver, section 79 will not apply to an intermediary if they have conspired, helped, abetted, or incited, whether by threats or promises.

CONCLUSION

India, one of the youngest countries in the world, has a sizeable population of children. According to this and who will be the future of this country, laws should be developed for the benefit of the children. There are many other forms of abuse that can happen to a young child. experiences, but sexual abuse is one of the most serious as it has a deep and long-lasting impact on the child. Consequently, legislation should be made to address this issue. The threat of cybercrime is now very serious for humanity. Prevention of cybercrime is essential for the social, cultural and security aspects of the country. The IT Act, 2000 was passed by the Government of India to address cyber crimes. Computers provide a new dimension to criminal law and present many challenges to law enforcement. The need for proper training to deal with these crimes is at the forefront of law enforcement concern. This requires additional resources. As we know that every coin has two sides, so basically in this article author is trying to tell that India is moving towards developed economy by which it is digitalizing itself and helping the world. Is using advanced means to win and also leading to more number of crimes. both positive and negative sides. Digital cashless economy depends heavily on technology. The author describes some of the legal issues related to cyberspace present in the present digital age. India is a lucrative market for many corporations due to its large population and scope for exponential growth. Thus stimulating the economy and examining specific problems or challenges. All the above analysis in this paper points towards increasing the level of execution of these laws related to cybercrime as the legislature has already endowed us with various provisions under various laws as proper execution is the only way to grow the economy and curb crimes. Can help reduce levels. excessive.

REFERENCES

1. www.indiacode.com
2. www.sodhganga.com
3. www.prsindia.org
4. www.indiankannon.org
5. Law journals.org
6. International journal of law